On multiplicative properties of difference sets

I. D. Shkredov

Steklov Mathematical Institute

Introduction

Let $\mathcal{R} = \mathcal{R}(+, \cdot)$ be a ring and $A, B \subseteq \mathcal{R}$ be any finite sets.

$$A + B := \{a + b \ : \ a \in A,\ b \in B\} \qquad \text{(sumset)}$$

$$A \cdot B := \{a \cdot b \ : \ a \in A,\ b \in B\} \qquad \text{(product set)}$$

General question

What can we say about the structure of sets S equal

$$A + B \quad \text{or} \quad A + A \quad \text{or} \quad A - A\ ?$$

$S = S + \{0\}$ or $S = (S + x) - \{x\}$, so we consider $|A|, |B| > 1$.

Fourier analysis and almost periodicity, I

We want to understand the structure of $A + B$.

Instead of studying the characteristic function of $A + B$ consider the function

$$f_{A,B}(x) = |A \cap (x - B)| = (1_A * 1_B)(x)$$

with the same support

$$\mathrm{supp}\, f_{A,B} = A + B\,.$$

We have

$$\widehat{f}_{A,B} = \widehat{1_A} \cdot \widehat{1_B}\,.$$

Fourier analysis and almost periodicity, I

Theorem (Croot–Sisask, 2010)

Let $\varepsilon \in (0,1)$, $K \geq 1$, $p \in \mathbb{N}$, $f : \mathbf{G} \to \mathbb{C}$ and

$$|A+A| \leq K|A|\,.$$

Then there is a set T, $|T| \geq |A| \exp(-O(\varepsilon^{-2} p \log |K|))$ s.t. $\forall t \in T$ one has

$$\|(f * 1_A)(x+t) - (f * 1_A)(x)\|_p \leq \varepsilon |A| \|f\|_p$$

In particular,

$$\|(1_B * 1_A)(x+t) - (1_B * 1_A)(x)\|_p \leq \varepsilon |A| |B|^{1/p}\,.$$

Fourier analysis and almost periodicity, I

In other words, $(1_B * 1_A)(x) \approx (1_B * 1_A)(x+t)$ for any $t \in T$.

By the triangle inequality

$$(1_B*1_A)(x) \approx (1_B*1_A)(x+t) \approx (1_B*1_A)(x+2t) \approx (1_B*1_A)(x+kt)$$

It implies that $A+B$ contains long arithmetic progressions.

Theorem (Croot–Laba–Sisask, 2011)

Let $A, B \subseteq \{1, 2, \dots, N\}$, $|A| = \alpha N$, $|B| = \beta N$. Then $A+B$ contains an arithmetic progression of length at least

$$\left(c \left(\frac{\alpha \log N}{(\log 2\beta^{-1})^3} \right)^{1/2} - \log(\beta^{-1} \log N) \right) .$$

One can find another structures in $A+B$:

uniformly distributed sequences,
large divisors (Sárközy, . . .)
and so on.

Works $\Leftrightarrow$ Fourier works $\Leftrightarrow$
works for sets with small ratio $|A+B|/|A|$, $|A+B|/|B|$.

Non almost periodicity approaches, II

Theorem (Croot–Ruzsa–Schoen, 2005)

Let $|A+A| \le K|A|$ or $|A-A| \le K|A|$. Then $A+A$ or $A-A$ contains an arithmetic progression of length at least

$$\log|A| / \log K \,.$$

Works for another structures as well (not only AP).

Sketch. We prove a weaker statement

$$A \subseteq \mathbb{F}_p, |A| \ge p/K \Rightarrow A - A \text{ contains AP of size}$$

$$\gg \log p / \log K \,.$$

Consider

$$S_j := A^k + j \cdot (1, 2, \dots, k) \subseteq \mathbb{F}_p^k\,, \qquad j = 0, 1, \dots, p-1\,.$$

We have $|S_j| = |A|^k$ and

$$\emptyset \neq S_i \cap S_j \Rightarrow (i-j) \cdot (1, 2, \dots, k) \in A^k - A^k = (A-A)^k\,.$$

If

$$|A|^k p > p^k \Leftrightarrow k \ll \log p / \log K$$

then $A - A$ contains an arithmetic progression of length k.

Non almost periodicity approaches, III

Katz–Koester's observation

Put $D := A - A$. Then

$$|D \cap (D + d)| \geq |A| + \varepsilon(d) \quad \text{for all } d \in D\,,$$

where $\varepsilon(d) \geq 0$.

Let us prove a simpler observation

$$|D\cap(D+d)| = |D\cap(D+a_1-a_2)| = |(D+a_1)\cap(D+a_2)| \geq |A|\,,$$

where $d = a_1 - a_2 \in D$.

We have

$$D = A - A = \bigcup_{a \in A} (A - a) \supseteq A - a, \qquad \forall a \in A\,.$$

and hence

$$A \subseteq (D + a_1) \cap (D + a_2)$$

for any $a_1, a_2 \in A$.

Katz–Koester

$$A - (A - a_1) \cap (A - a_2) \subseteq (D + a_1) \cap (D + a_2)$$

Non almost periodicity approaches, III

From Katz–Koester's observation the number of solutions of

$$x + y = z\,, \qquad x, y, z \in D = A - A$$

is at least $|A||D|$. This bound is optimal.

Theorem (Shkredov, 2014)

The number of solutions of

$$x - x' = y - y' = z - z'\,, \qquad x, y, z \in D = A - A$$

is at least $|D|^{7/4}|A|^{9/4}$.

We do not know is this optimal or not. Other equations.

Can a sumset be a multiplicative subgroup?

If we believe that sumsets have some *additive* structure then can we prove that any *multiplicatively* rich set, say, a multiplicative subgroup, is not a sumset?

Answer: not yet, this is complicated.

Conjecture (Sárközy, 2012)

Let $R \subset \mathbb{F}_p$ be the set of all quadratic residues. Is it true that

$$R \neq A + B \qquad \forall A, B, \quad |A|, |B| > 1?$$

Shkredov (2014) : yes, for $A = B$.

Theorem (Shparlinski, 2013)

Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup and for some $A, B \subseteq \mathbb{F}_p$ one has

$$A + B \subseteq \Gamma\,,$$

where $|A|, |B| > 1$. Then

$$|A|,\, |B| \le |\Gamma|^{1/2+o(1)}$$

as $|\Gamma| \to \infty$. In particular, if $A + B = \Gamma$ then

$$|A|,\, |B| = |\Gamma|^{1/2+o(1)}\,.$$

Sárközy: $\Gamma = R$.
Shkredov: $\Gamma = R$, slightly another method and better bounds.

Let $S = A + B$. We know that

$$A \subseteq (S - b_1) \cap (S - b_2)$$

for any $b_1, b_2 \in B$.

A generalization

$$A \subseteq (S - b_1) \cap (S - b_2) \cap \cdots \cap (S - b_k)$$

for any $b_1, b_2, \ldots, b_k \in B$.

$$A \subseteq (S - b_1) \cap (S - b_2) \cap \dots \cap (S - b_k)\,.$$

If $S = R$ then by Weil's bound

$$|(R + x_1) \cap (R + x_2) \cap \dots \cap (R + x_k)| \ll_k p^{1/2+o(1)}\,.$$

For smaller subgroups Stepanov's method works

Theorem (Vyugin–Shkredov, 2012)

Let Γ be a subgroup, $|\Gamma| < p^{1-\varepsilon}$. Then for any x_j

$$|(\Gamma + x_1) \cap (\Gamma + x_2) \cap \dots \cap (\Gamma + x_k)| \ll_k |\Gamma|^{1/2+o(1)}\,.$$

Theorem (Shkredov, 2015)

Let Γ be a subgroup, $|\Gamma| < p^{1/2-\varepsilon}$. Then

$$\Gamma \neq A + B\,,$$

where A is another subgroup and B is an arbitrary set.

Theorem (Shkredov, 2016)

Let Γ be a subgroup, $|\Gamma| < p^{3/4-\varepsilon}$. Then

$$\Gamma \neq A - A\,,$$

where A is an arbitrary set.

The necessary condition: real case

Put $D = A - A$.

Theorem (Roche–Newton—Zhelezov, 2015)

Let $A \subset \mathbb{R}$ be a finite set, and $\varepsilon > 0$ be a real number. Then for some constant $C'(\varepsilon) > 0$ one has

$$|DD|, |D/D| \gg_{\varepsilon} |D| \cdot \exp(C'(\varepsilon) \log^{1/3-o(1)} |D|) .$$

Theorem (Shkredov, 2016)

Let $A \subset \mathbb{R}$ be a finite set. Put $D = A - A$. Then

$$|DD|, |D/D| \gg |D|^{1+\frac{1}{12}} \log^{-\frac{1}{4}} |D| .$$

Thus, say, $\{1, 2, 2^2, 2^3, \dots, 2^n\}$ is not a difference set.

Theorem (Shkredov, 2015)

Let $A \subset \mathbb{F}_p$ be a set. Put $D = A - A$, $|D| < p^{4/7}$. Then

$$|DD|,\ |D/D| \gg |D|^{19/24}|A|^{3/8}\,.$$

Again, the product set and the quotient set of D are large. Hence

Theorem (Shkredov, 2016)

Let Γ be a subgroup, $|\Gamma| < p^{3/4-\varepsilon}$. Then

$$\Gamma \neq A - A\,,$$

where A is an arbitrary set.

Sketch of the proof

For any A consider the set

$$R[A] = \left\{ \frac{a_1 - a}{a_2 - a} \;:\; a, a_1, a_2 \in A,\ a_2 \neq a \right\} \subseteq D/D\,.$$

Theorem (Jones, 2013 and Roche–Newton, 2015)

We have

$$|R[A]| \gg \frac{|A|^2}{\log |A|} \geq |D|^{1-o(1)}\,.$$

Theorem (Aksoy–Murphy–Rudnev–Shkredov, 2015)

For any $A \subseteq \mathbb{F}_p$, $|A| < p^{2/3}$ one has

$$|R[A]| \gg |A|^{3/2}\,.$$

A crucial observation

$$R[A] = \left\{ \frac{a_1 - a}{a_2 - a} \;:\; a, a_1, a_2 \in A,\ a_2 \neq a \right\} \subseteq D/D\,.$$

We have

$$1 - \frac{a_1 - a}{a_2 - a} = \frac{a_2 - a_1}{a_2 - a} = \frac{a_1 - a_2}{a - a_2} \in R[A]\,,$$

and thus

$$R[A] = 1 - R[A]\,.$$

So, $R[A]$ is *additively* structured.

General sum–product

General principle

If A belongs to a ring $\mathcal{R}(+,\cdot)$ and

$$|A+A|, |AA| \ll |A|^{1+\varepsilon}$$

then A has "large" intersection with a subring.

Finite fields of prime order (Bourgain, Katz, Tao, Konyagin, Glibichuk, Chang, Garaev, Rudnev, Li, Roche–Newton, Shkredov, ...)

Infinite fields and rings (Erdös, Szemerédi, Chang, Solymosi, Konyagin, Rudnev, Roche–Newton, Shkredov, ...).

Applications: Number Theory, Cryptography, Additive Combinatorics, Computer Science, Dynamical Systems.

Sum–product in $\mathbb{R}$ and $\mathbb{F}_p$

The real case.

Theorem (Konyagin–Shkredov, 2016)

Let $A \subset \mathbb{R}$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{4/3+c},$$

where $c > 0$ is an absolute constant.

The prime fields case.

Theorem (Roche-Newton–Rudnev–Shkredov, 2015)

Let $A \subset \mathbb{F}_p$, $|A| < p^{5/8}$ Then

$$\max\{|A+A|, |AA|\} \gg |A|^{1+1/5}.$$

By sum–product we know that a set cannot has good multiplicative and additive structure simultaneously.

Lemma (a variant of sum–product phenomenon)

For any $A, B \subset \mathbb{R}$ and nonzero α, we have

$$|A \cap (B + \alpha)| \ll |A|^{-2/3} |AB|^{4/3} .$$

E.g. $A = B$ and $|AA| \ll |A|$. Then $|A \cap (A + \alpha)| \ll |A|^{2/3}$, $\alpha \neq 0$.

Similar (but more complicated) result in $\mathbb{F}_p$ takes place.

Let $R = R[A]$. By our main observation

$$|R| = |R \cap (1-R)| \ll |R|^{-2/3} |RR|^{4/3} .$$

Hence ($R \subseteq D/D$)

$$|DD/DD| \ge |RR| \gg |R|^{5/4} \gg |D|^{5/4 - o(1)} .$$

By some standard tools (Plünnecke inequality), we have

$$|DD|, |D/D| \gg |D|^{1+c} ,$$

where $c > 0$ is an absolute constant.

Problems

Problem 1. It is known that

$$|D|^{3/2} \gg |DD| \gg |D|^{1+c},$$

where $c = 1/8 - o(1)$. What is the right exponent?

Problem 2. Recall

$$R[A] = \left\{ \frac{a_1 - a}{a_2 - a} \;:\; a, a_1, a_2 \in A,\ a_2 \neq a \right\} \subseteq D/D\,.$$

Is it true $R[A] \gg |A - A|$, $R[A] \gg |A/A|$?

Problem 3. $S \subset \mathbb{F}_p$, $|S| \le p/2$ is a perfect difference set iff the number of solutions of the equation $x = s_1 - s_2$, $s_1, s_2 \in S$, $x \neq 0$ does not depend on x.

Is it true that $S \neq A - A$?

Problem 4 (P. Hegarty) A set $S = \{s_1 < s_2 < \cdots < s_n\}$ is called strictly *convex* if the consecutive differences $s_i - s_{i-1}$ are strictly increasing.

Let $S \subseteq A + A$ and S be a strictly convex (concave) set. Is it true that $|S| = o(|A|^2)$?

Thank you for your attention!